

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

AFFINITY CREDIT UNION, et al.,
Plaintiffs,
v.
APPLE INC.,
Defendant.

Case No. [22-cv-04174-JSW](#)

**ORDER RESOLVING DISCOVERY
DISPUTES**

Re: Dkt. No. 72

Now before the Court for consideration is the Joint Letter Brief regarding Disputed Provisions of Proposed Protective Order and Protocol for Electronically Stored Information (“ESI Protocol”). (Dkt. No. 72.) The Court finds the matter appropriate for resolution without further briefing or telephone conference. *See* Civ. L.R. 7-1(b); Civil Standing Order No. 7.

Plaintiffs Affinity Credit Union, Greenstate Credit Union, and Consumers Co-Op Credit Union (“Plaintiffs”) and Defendant Apple Inc. (“Apple”) have submitted competing proposed Protective Orders and ESI Protocols. Although the competing proposed orders are substantially identical, Plaintiffs believe Apple’s desired security and confidentiality measures go too far. Apple counters that stringent measures are necessary because hackers increasingly target law firms to access confidential information, and it fears that certain documents could be used by Plaintiffs to gain commercial advantage in future negotiations.

The parties’ dispute seemingly places in conflict two important concerns: on the one hand, expeditiously litigating this putative class action, and, on the other, safeguarding the parties (and innocent non-parties) from disclosure and misuse of their private information. Resolution is much simpler than this dispute would suggest because the least restrictive measures proposed by Plaintiffs operate to further Apple’s privacy goals. The Court addresses each dispute below, and it

enters the final Protective Order and ESI Protocol in subsequent docket entries.

A. The Court Adopts Provisions from Each of the Proposed Protective Orders.

The parties disagree regarding one issue in Section 9 and two issues in Section 11 of the proposed Protective Orders. As discussed below, the Court adopts language from each of the parties' proposals.

1. The Court Approves Apple's Language Regarding Discovery Material Designated As "Highly Confidential – Attorneys' Eyes Only."

The parties agree to include a category of confidential document production for "Highly Confidential" information that "is extremely confidential and/or sensitive in nature and [that] the Producing Party reasonably believes . . . is likely to (1) cause economic harm or significant competitive disadvantage to the Producing Party or (2) reveal personal identifiable information." (Dkt. No. 72-1, at 1.) Apple seeks to make this category "Attorneys' Eyes Only," meaning that no client representatives may view the information. Plaintiffs propose permitting up to three client representatives and their immediate staff to access Highly Confidential materials.

Apple argues that Plaintiffs may use the Highly Confidential materials for improper purposes, including in future negotiations with Apple. Plaintiffs contend that Apple's concern lacks a reasonable basis because Plaintiffs and Apple are not competitors and because Apple uses standardized terms for all issuer banks.

While Plaintiffs' position has merit, the proposed "Highly Confidential" definition only relates to materials that could "cause economic harm or significant competitive disadvantage." Because Plaintiffs and Apple are not competitors, and because Apple uses standardized terms, this definition cannot realistically cover a significant number of materials that impact Plaintiffs' ability to assess the strengths and weaknesses of their case. The Court would be skeptical if the "Highly Confidential" designation were used more than sparingly to shield competitive information.

The Court thus adopts Apple's proposed language limiting this category to Attorneys' Eyes Only. Plaintiffs may challenge the designation of some or all of the materials as Highly Confidential at a later date if Plaintiffs have a good faith basis to believe the designations are improper.

2. The Court Approves Plaintiffs' Language Regarding Data Security.

Apple seeks an order requiring the parties to comply with one of three strict security protocols, reasoning that the trend in recent years has been for firms and courts to require stricter measures. Apple also requests language requiring multi-factor authentication for access to confidential materials. Plaintiffs argue that Apple's cybersecurity protocols are impractical and expensive. They point out that, in the only identified similar case involving Apple's proposed protocols, the plaintiffs and their experts spent 250 hours over the course of eight weeks to implement the protocols. (Dkt. No. 72, at 3.) Finally, Plaintiffs assert that Apple's proposed language regarding multi-factor authentication is overbroad and ambiguous.

Apple's proposed language is a departure from the Model Protective Order for this District. Although the trend may be to adopt increasingly strict cybersecurity protocols, the Court finds that Plaintiffs' proposed language is more than sufficient. Where the Model Protective Order requires Protected Material to be "stored and maintained. . . in a secure manner," (*see* "Model Protective Order for Standard Litigation," ¶ 7.1, available at <https://www.cand.uscourts.gov/forms/model-protective-orders/>), Plaintiff's proposed language goes above and beyond: It requires the Receiving Party to "implement an information security management system ("ISMS"), including reasonable and appropriate administrative, physical, and technical safeguards and network security and encryption technologies governed by written policies and procedures, designed to protect against any reasonably anticipated threats or hazards to the security of such Protected Material and to protect against unauthorized access to Protected Material." (Dkt. No. 72-1, at 3.) This is more than sufficient.

The Court also finds Plaintiffs' language regarding multi-factor authentication to be sufficient. Apple's proposed language of "for any access" is vague, and it is unclear how the Court would enforce the provision. It is unclear to the Court if, for example, authentication would be required when opening every draft of a brief or letter, or if authentication when logging into one's computer is sufficient. Plaintiffs' language of "to prevent unauthorized access" is judicially administrable: if a breach occurs because an access point lacked multi-factor authentication, the party or parties did not comply with the multi-factor authentication provision.

3. The Court Adopts Plaintiffs' Language Regarding Data Breach Discovery.

The parties define a "Data Breach" as including "any cyberattack or other deliberate security breach. . . including as a result of or following an inadvertent disclosure." (Dkt. No. 72-1, at 4.) In the event of a Data Breach, "the Parties shall meet and confer in good faith regarding any adjustments that should be made to the discovery process and discovery schedule in this action." (*Id.* at 5.) Apple seeks the following language be added: "Further, the Receiving Party shall submit to reasonable discovery concerning the Data Breach." (*Id.*)

Apple contends that its proposed language is reasonable, appropriate, and fulfills the purpose of the protective order. Plaintiffs respond that it is unreasonable to mandate data breach discovery and assert that a party can make an application for discovery if a breach occurs.

The Court is concerned that Apple's language would invite satellite disputes unrelated to resolution of this action. Moreover, Section 11(c) of the proposed Protective Orders requires compliance with "reasonable request(s) that Receiving Party investigate, remediate, and mitigate the effects of a Data Breach. . . [and] promptly provide any information that is reasonably requested by Producing Party and that relates to any such Data Breach. . . ." (*Id.* at 4.) If this informal discovery is insufficient, the Producing Party can seek leave to conduct formal discovery from the Court.

4. Leave of Court Is Required to File Documents Under Seal.

The Court *sua sponte* modifies Section 1 and Section 13 of the Protective Order. No documents may be filed under seal without prior authorization from the Court, consistent with the Civil Local Rules.

B. The Court Approves Plaintiffs' ESI Protocol.

Apple seeks to add language to the ESI Protocol as follows: "With respect to privileged or work-product information involving **in-house or** outside litigation counsel in this action and generated after the filing of the complaint, parties are not required to include any such information in privilege logs." (Dkt. No. 72-1 at 7, proposed language in bold.) Apple argues that there is no principled distinction between in-house and outside communications because Apple employs in-house dedicated commercial litigators. Apple also argues that logging in-house communications

would be unduly burdensome and have a “chilling effect” on attorney-client communications.

Plaintiffs argue that Apple has no basis to unilaterally designate in-house counsel as litigation counsel. Plaintiffs assert that Apple has a history of including in-house counsel on business emails to create a false appearance of privilege, and they argue that requiring a privilege log would protect against excessive claims of privilege and would not be unduly burdensome. Plaintiffs also point out that they attempted to reach compromise with Apple by seeking the names of in-house litigation counsel whose communications and work product could properly be withheld from the privilege log, and Apple refused.

1. Legal Standards Pertaining to Attorney-Client Communications.

The attorney-client privilege protects confidential communications made by clients to their attorneys to obtain legal advice and the attorneys’ advice in response. *United States v. Ruehle*, 583 F.3d 600, 607 (9th Cir. 2009). “The fact that a person is a lawyer does not make all communications with that person privileged.” *Id.* (quoting *United States v. Martin*, 278 F.3d 988, 999 (9th Cir. 2002)).

“In the corporate context, courts have recognized that in-house counsel is often involved in the day-to-day operation of the company.” *L.D. v. United Behav. Health*, No. 20CV02254YGRJCS, 2022 WL 3139520, at *13 (N.D. Cal. Aug. 5, 2022). “Because communications with in-house counsel relating only to the business operations of the company are not protected by attorney-client privilege, a client seeking to protect communications between a corporate client and in-house counsel must ‘make a clear showing that in-house counsel’s advice was given in a professional legal capacity.’” *Id.* (quoting *United States v. Chevron Corp.*, No. C-94-1885 SBA, 1996 WL 264769, at *4 (N.D. Cal. Mar. 13, 1996)).

The Ninth Circuit has articulated an eight-part test to determine whether information is covered by the privilege:

(1) Where legal advice of any kind is sought (2) from a professional legal adviser in his capacity as such, (3) the communications relating to that purpose, (4) made in confidence (5) by the client, (6) are at his instance permanently protected (7) from disclosure by himself or by the legal adviser, (8) unless the protection be waived.

Ruehle, 583 F.3d at 607 (quoting *In re Grand Jury Investigation*, 974 F.2d 1068, 1071 n.2 (9th

1 Cir. 1992)). The party asserting the privilege has the burden of establishing that the
 2 communications are privileged “and, if necessary, to segregate the privileged information from the
 3 non-privileged information.” *Id.* at 609. The production of a privilege log is a well-established
 4 means by which a party asserting privilege can make a *prima facie* showing that the information is
 5 protected. *In re Grand Jury Investigation*, 974 F.2d at 1070-71.

6 Courts in this circuit typically do not require litigants to produce a privilege log for
 7 communications and work product made after litigation commences. *In re Snap Inc. Sec. Litig.*,
 8 No. CV1703679SVWAGRX, 2018 WL 7501294, at *1 (C.D. Cal. Nov. 29, 2018). However,
 9 there is no consensus on whether such logs are required by Federal Rule of Civil Procedure
 10 26(b)(5)(A) and whether a distinction between in-house counsel and outside counsel is warranted.
 11 *See Weiland Sliding Doors & Windows, Inc. v. Panda Windows & Doors, LLC*, No. 10CV0677
 12 JLS (MDD), 2011 WL 13100735, at *3 (S.D. Cal. June 23, 2011) (noting lack of consensus and
 13 declining to require privilege logs for post-litigation communications where continuing conduct
 14 was not at issue).

15 **2. Apple Has Not Made a “Clear Showing” That In-House Counsel**
 16 **Communications Would Be Made in Furtherance of Providing Legal Advice.**

17 Apple has not met its burden to make a *prima facie* showing that communications with its
 18 in-house counsel may be withheld without logging. It fails to meet prongs (2) and (3) of the
 19 privilege test, because it is unclear that in-house counsel for Apple are acting “in their capacity” as
 20 legal advisors or that the withheld communications “relate to that purpose.” *See Ruehle*, 583 F.3d
 21 at 607. As Apple recognizes, there may be a “general practice,” not specific to Apple, “of
 22 business people including a lawyer in an email chain in the incorrect belief that doing so makes
 23 the email privileged.” (Dkt. No. 72, at 8 (internal quotations omitted).) Providing a privilege log
 24 will permit Plaintiffs to assess whether communications are made for legal advice or pursuant to
 25 Apple’s ordinary business practice.

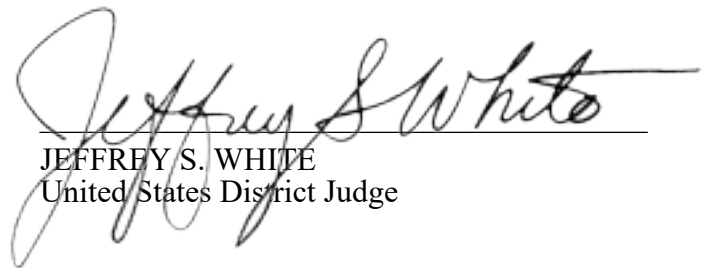
26 The Court further agrees with Plaintiffs that a compromise to ease the burden of producing
 27 a privilege log is possible in the event Apple identifies specific in-house litigation counsel whose
 28 communications would be entitled to the presumption of privilege without logging. Such a list

1 would not, as Apple claims, “restrict [its] ability to assess documents individually” or
2 “presuppose[Apple’s] wrongdoing.” (*Id.* at 8 n.38.) Apple has the same obligation to assess
3 responsive communications with or without such a list; the sole difference the list would provide
4 is that Apple would not have the burden of including privileged communications from the listed
5 individuals in the privilege log.

6 Accordingly, the Court adopts Plaintiff’s ESI Protocol in full. Apple may move to enter an
7 amended ESI protocol in the event the parties reach a compromise regarding the privilege log.

8 **IT IS SO ORDERED.**

9 Dated: March 29, 2024


JEFFREY S. WHITE
United States District Judge